**IN THE**

**UNITED STATES PATENT AND TRADEMARK OFFICE**

| | |
|---|---|
| APPLICANT: | Milo S. Medin |
| SERIAL NO.: | 08/811,586 |
| FILING DATE: | March 5, 1997 |
| TITLE: | SYSTEM AND METHOD FOR DELIVERING HIGH-PERFORMANCE ONLINE MULTIMEDIA SERVICES |
| EXAMINER: | W. Vaughn, Jr. |
| GROUP ART UNIT: | 2756 |
| ATTY. DKT. NO.: | 2617 |

Revised Declaration of Milo S. Medin

I, Milo S. Medin, hereby declare the following:

1. I am the sole inventor of the invention described and claimed in U.S. Patent Application Serial No. 08/811,586, entitled "System and Method for Delivering High-Performance Online Multimedia Services," filed on March 5, 1997. I am providing this declaration to antedate the patents and other references cited by the Examiner in the Office Actions mailed April 1, 1999, November 24, 1999, and November 20, 2000 as listed below.

| Patent Number/Author & Title | Filing Date | Issue/Publication Date |
|---|---|---|
| 5,838,927 | November 22, 1996 | November 17, 1998 |
| Baentsch et al. | N/A | May 1996 |
| Jeffrey et al. | N/A | May 1996 (as best able to determine) |
| 5,727,159 | April 10, 1996 | March 10, 1998 |
| 5,768,528 | May 24, 1996 | June 16, 1998 |
| 5,787,470 | October 18, 1996 | July 28, 1998 |

| | | |
|---|---|---|
| 5,864,852 | April 26, 1996 | January 26, 1999 |
| 5,935,207 | April 9, 1997 (parent: June 3, 1996) | August 10, 1999 |
| 5,940,074 | November 22, 1996 (parents: June 3, 1996) | August 17, 1999 |
| 5,956,716 | June 7, 1996 (parent: June 7, 1995) | September 21, 1999 |

2. I am currently the Senior Vice President of Engineering and Chief Technical Officer ("CTO") for @Home Networks, Inc. ("@Home"), having an office at 425 Broadway, Redwood City, CA 94063. I have been employed at @Home since June, 1995 and at that time had the title of Vice President, Networks. My duties as Vice President included the design and implementation of @Home's network architecture.

3. Attached hereto as Exhibit A are selected sections of a document entitled "Router and Switch Request for Proposal" (the "RFP"), which was completed by at least January 26, 1996. I supervised the preparation of the RFP and the @Home network architecture described therein is my own invention.

4. The RFP was confidentially distributed to manufacturers and vendors to solicit architectural details and pricing information for routers and switches. @Home did not offer to sell the @Home network architecture described in the RFP to the manufacturers and vendors. Rather, @Home solicited the details and information because @Home desired to purchase routers and switches in order to implement the @Home network architecture described in the RFP.

5. As stated in Section 3.5 of the RFP, the RFP defined particular technical, administrative, or operational specifications, features, functions, limitations, restrictions, and performance parameters that were necessary to satisfy the minimum overall operational and service performance criteria for the routers and switches. As such, the

RFP had to be complete and specific as to architectural details and functional operations of the @Home network architecture.

6. The RFP describes an embodiment of the invention described and claimed in the Application. For example, Section 7 of the RFP describes a technical overview of the @Home network architecture, including an embodiment of the claimed invention. Numerous figures are included in the RFP to aid in the understanding of the described system.

7. The information in the RFP is sufficient to allow myself and others with ordinary skill in the art to directly implement the claimed system and method for delivering high-performance online multimedia services. Moreover, the @Home network, which is commercially available today, was built in conformance with the @Home network architecture described in the RFP.

8. Independent claims 1, 12, 13, and 17 collectively recite a system and method for delivery of high-performance online multimedia services. Independent claims 24 and 31 respectively recite a method and system for replicating content from a content provider.

9. Claims 1, 12, and 31 recite "a high-speed backbone coupled to a plurality of network access points of a publicly accessible internetwork of networks..." Claim 24 similarly recites "a private network." The RFP includes FIG. 1, entitled "@Home Network Architecture," which illustrates a component labeled "@Home Private ATM Backbone." FIG. 2 of the RFP, entitled "@Home Backbone Network Architecture," which illustrates components labeled "@Home Backbone Carrier ATM Network" and "Backbone Router." Section 7.1 refers to the illustrated @Home backbone as a "multi-megabit switched data system," which is high-speed network. Thus, the backbone

illustrated in FIGS. 1 and 2 is an embodiment of the claimed high-speed backbone and private network. FIGS. 1 and 2 further illustrate that the backbone is coupled to a "Global Internet" (a publicly accessible internetwork of networks) by a plurality of network access points ("NAPs"). FIG. 2, for example, lists exemplary NAPs including "MAE-West," "@Sprint-NAP," and "@MAE-East" and includes a detailed drawing of the hardware comprising a NAP.

10. Claim 1 further recites a "plurality of regional servers coupled to the high-speed backbone via routers, each regional server for providing a second level of caching of the content for a region." Claim 12 recites a "plurality of regional servers coupled to the high-speed backbone via routers, where content is replicated amongst the regional servers." Claim 24 similarly recites a "first regional server" and a "plurality of peer regional servers coupled to the first regional server via the private network." Likewise, claim 31 recites "a plurality of regional servers coupled to the high-speed backbone for retrieving the content provided by the content provider." Claims 24 and 31 also recite that "content retrieved by one of the regional servers is replicated to the other regional servers via the high-speed backbone" (quoting from claim 31). Embodiments of the claimed regional servers are fully described throughout Section 7. Specifically, FIGS. 1 and 2 show "Regional Networks" coupling "Regional Data Centers" ("RDCs") to the backbone. FIG. 6 illustrates the servers, switch, and routers forming the RDC. Section 7.4 describes how a RDC houses high-availability servers for providing World Wide Web access, email, news, and other features. The caching and replication properties of the regional servers are described in Section 7.1, which states that @Home's network "is

based on a distributed model" and makes "extensive use of caching and replication to minimize traffic on the system's backbone."

11. Claim 1 also recites "a plurality of caching servers in modified head-ends coupled to each of the regional servers..." Section 7.5 explicitly states that WWW caching proxy servers are stored at a cable headend facility and coupled via a router to the regional network. These WWW caching proxy servers are embodiments of the claimed caching servers.

12. Finally, claim 1 recites "a broadband distribution network coupling each of the caching servers to a plurality of end-user systems..." FIG. 7 and its associated text in Section 7.5 describe how the illustrated caching servers are coupled to cable routers via a fast Ethernet switch. The cable routers are coupled to end-user systems ("User Homes") via the cable plant. These components comprise one embodiment of the claimed broadband distribution network.

13. Independent claims 12 and 17 respectively recite a system and method for multicasting content. Claim 12 recites multicasting content from a regional server to a group of end-user systems. Claim 17, similarly, recites the steps of multicasting general content to a multicast destination address, customizing the general content to suit an area, and multicasting the customized content to that area. The RFP describes the multicasting properties of the @Home network architecture beginning in Section 4. This section, entitled "Related and Cited Documents," refers to various multicasting documents, including "Host Extensions for IP Multicasting (IGMP Version 1), RFC 1112," "Multicast Extensions to OSPF, RFC 1584," "Protocol Independent Multicast (PIM): Protocol Specification (1/11/1995)," and "Protocol Independent Multicast-Sparse Mode

(PIM-SM): Protocol Specification (9/7/95)." In addition, a subheading in Section 8.1.5, "Multicast," describes how the routers must implement IP multicasting. Section 8.2.5 outlines similar multicasting requirements. Thus, it is implicit in the design of the network that multicasting will be performed from the regional servers to the end-user systems. Section 7.1 describes how content providers will "create multimedia content that takes advantage of the high-speed network, as well as extensive local news and information." This latter text suggests that general content will be supplemented with local content (the "local news and information") and multicast to a local area, as claimed. Thus, the RFP describes an embodiment of the claimed system and method for multicasting.

14. Claim 12 additionally recites "a central server coupled to the high-speed backbone" having a network management system. As described above, FIG. 6 illustrates a RDC coupled to the backbone network. A plurality of servers are illustrated in the RDC and the text in Section 7.4 mentions that these servers can be used for "WWW, email, news, DHCP, etc." Thus, these servers are embodiments of the claimed central server. A network management system can be executed on one of these servers. Indeed, in Section 8.2.1, requirement 92 (R:92) states that a RDC device "must include both in-band and out-of-band mechanisms to allow the *network manager* to reload, stop, and restart the device." Thus, the RFP expects a network manager to be executing in a RDC, and thereby describes an embodiment of the claimed network management system.

15. Dependent claim 7 recites "a coupling from a remote local area network to the high-speed backbone which bypasses the publicly accessible internetwork of networks. Similarly, dependent claims 28 and 35 recite a content provider coupled to the private

network via a direct connection. FIG. 1 of the RFP illustrates "Off-net Tailsites" including "Content Providers" coupled directly to the @Home Private ATM Backbone and Regional Network. The associated text in Section 7.1 of the RFP states that "The @Home backbone and regional networks would also serve tailsites, including content providers..." FIG. 5 also shows a Regional Router coupling the Regional Network to a Tailsite. Thus, the RFP illustrates a content provider coupled directly to the private network.

16. The independent claims and/or claim elements not specifically described above correspond to claims and/or claim elements that were described above. Accordingly, the invention described and claimed in the Application was completed by at least January 26, 1996.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

8/1/01
Date

Milo S. Medin

# EXHIBIT A

# Router and Switch Request For Proposal

*This document is the Confidential Property of @Home.*

## 3.1 @Home's Obligations

@Home shall not incur any obligation or liability whatsoever by reason of issuance of the RFP. This document does not constitute an offer to purchase or a commitment by @Home to purchase any equipment or services. All of the plans and intentions discussed in the RFP are for information purposes only and may change as @Home's needs dictate. @Home shall not be responsible for or pay any expenses or losses which may be incurred by a vendor in preparing and submitting its proposal or taking any other actions. These expenses or losses will be borne solely by the vendor. All material submitted in response to this RFP will become the property of @Home.

@Home reserves the right to make no, partial, or full awards for whatever reasons it deems appropriate. Additionally, @Home reserves the right to subsequently modify any award based on the vendor's performance and/or @Home's business needs. @Home reserves the right to enter negotiations, and contract, with more than one vendor if such arrangements are deemed to be in @Home's best interest.

## 3.2 Confidentiality

### 3.2.1 Confidential Information

In the course of the selection process, it may be necessary for @Home and vendors to exchange Confidential Information. For the purposes of this RFP, "Confidential Information" shall mean the existence and terms of this RFP and any information disclosed by @Home to a vendor or from a vendor to @Home, in the following forms, during the period of time commencing on the date of this RFP and ending one year later:

- if in written, graphic, machine-readable or any other tangible medium, to the extent conspicuously marked with a "confidential," "proprietary" or similar legend; and
- if originally disclosed orally or by way of observation, to the extent identified as Confidential Information at the time of such original disclosure and to the extent summarized in reasonable detail and confirmed as being Confidential Information in a written notice delivered to the receiving party within 30 days after original disclosure, which notice includes a reference to the date of the original disclosure and a reference to this RFP.

### 3.2.2 Exceptions

Confidential Information shall not include information which:

- was acquired by the receiving party prior to the time of its disclosure by the disclosing party, as shown by files of the receiving party in existence at the time of disclosure, and at a time when the receiving party was under no obligation to the disclosing party to keep such information confidential;
- is or becomes available in the public domain through no wrongful act of the receiving party;
- is received by the receiving party from a third person or entity that is not known by the receiving party to be sharing such information in violation of rights of the disclosing party;
- is developed by or on behalf of the receiving party without any use of Confidential Information of the disclosing party; or

- is at any time furnished to a third party by the disclosing party without restrictions on the third party's rights to disclose.

The party claiming that any of the foregoing exceptions applies shall have the burden of proving such applicability.

### 3.2.3 Obligations

@Home (with respect to Confidential Information of a vendor) and each vendor (with respect to Confidential Information of @Home) shall take the following actions, for a period of time commencing on the date of this RFP and ending two years thereafter:

- treat Confidential Information of the other party with the same degree of confidentiality with which it treats its own Confidential Information, in no case less than a reasonable degree of confidentiality;
- use Confidential Information (in the vendor's case) only for the purposes of responding to the RFP, or (in @Home's case) only for the purposes of evaluating the Confidential Information and determining whether to pursue further negotiations with the applicable vendor;
- refrain from copying Confidential Information, in whole or in part, except as required in furtherance of the uses thereof permitted hereunder, and except with accurate reproduction of all proprietary legends and notices located in the originals;
- limit dissemination of Confidential Information to only those of such employees and agents of the receiving party (and in cases where @Home is the receiving party, employees and agents of (i) @Home, (ii) shareholders of @Home, and (iii) cable television and other network operators that may offer the @Home service to their customers) who have a need to know the Confidential Information in furtherance of the uses thereof permitted hereunder; provided, however, that a receiving party shall in all events be responsible to the disclosing party for any action or inaction of the receiving party's employees, agents and former employees and agents that would violate this Agreement, had the action or inaction been that of the receiving party directly; and
- destroy or return to the disclosing party any Confidential Information received in written or other tangible media, including all copies and records thereof, upon any request by the disclosing party, except for a single set of copies which the receiving party may retain solely as an archival record of materials submitted.

### 3.2.4 Legally Required Disclosure

If either of @Home or any vendor, or any of its representatives becomes compelled to disclose any Confidential Information of the other pursuant to applicable laws, rules or regulations, or pursuant to applicable stock exchange or stock association rules (collectively, the "Requirements") the receiving party shall provide the disclosing party with prompt notice of such Requirements and shall cooperate with the disclosing party in seeking to obtain any protective order or other arrangement pursuant to which the confidentiality of the Confidential Information is preserved. If such an order or arrangement is not obtained, the receiving party agrees that it and its representatives will disclose only that portion of the Confidential Information as is required pursuant to such Requirements. Any such required disclosure shall not, in and of itself, change the status of the disclosed information as Confidential Information under the terms of this RFP.

### 3.2.5 Acknowledgment

BY ACCEPTING AND, FURTHER, BY RESPONDING TO THIS RFP, EACH VENDOR ACKNOWLEDGES AND AGREES THAT, SUBJECT TO THE TERMS OF ANY SEPARATE NON-DISCLOSURE AGREEMENT IN EFFECT BETWEEN @HOME AND SUCH VENDOR, IT IS FULLY BOUND BY ALL OF THE PROVISIONS OF THIS RFP, INCLUDING BUT NOT LIMITED TO THE PROVISIONS IN THIS SECTION 3.2,

NOTWITHSTANDING ANY LEGENDS OR OTHER COMMUNICATIONS TO THE CONTRARY THAT MAY ACCOMPANY SUCH VENDOR'S RESPONSE.

### 3.3 Intellectual Property Rights

It is the responsibility of the vendor to obtain all necessary intellectual property rights for all equipment, software, systems, and methods proposed. This includes but is not limited to patents, copyrights, and trade secrets. In addition, vendor teams shall identify, within their proposal, any proprietary technology embodied in the equipment and/or software proposed in response to the RFP. Vendor teams shall indemnify, defend and hold harmless @Home from and against all expenses (including attorneys' fees) and liability arising from lawsuits and other claims that allege infringement, violation or misappropriation of any patent, copyright, trade secret or any other intellectual property right based on @Home's making, having made, using or selling of the vendor's products.

### 3.4 Federal, State, and Local Regulations

All vendor proposed hardware, software, equipment, materials and components comprising all subsystems must meet or exceed all applicable FCC, EIA, ANSI, UL, and all other federal, state and local regulations for deployment at the contemplated service venues.

### 3.5 Requirements Terminology

Requirements define a particular technical, administrative, or operational specification, feature, function, limitation, restriction, or performance parameter that is necessary to satisfy the minimum overall operational and service performance criteria for the routers and switches.

Failure to meet a requirement may cause unacceptable service application restrictions, improper functioning of equipment, hindrance of service operations to an unacceptable level, or unacceptable performance, and such failure is grounds for rejection of a router/switch.

All specifications set forth herein are to be construed as requirements unless otherwise stated.

In the event of conflicting specifications, the more stringent shall govern.

## *4. Related and Cited Documents*

The following reference documents are related to the requirements in this RFP and may be cited within this document.

1) Requirements for IP Version 4 Routers, RFC 1812
2) Requirements for Internet Hosts, RFC's 1122,1123
3) SNMP protocol standard, RFC's 1155, 1156, 1157, 1213, 1212, 1215
4) Type of Service in the Internet Protocol Suite, RFC's 1340,1349
5) Service Mappings, (IP Precedence) RFC 795
6) Dynamic Host Configuration Protocol (DHCP), RFC 1541,1533,1532
7) DHCP Options and BOOTP Vendor Information Extensions, RFC 1533
8) Assigned Numbers, RFC 1700
9) Host Extensions for IP Multicasting (IGMP Version 1), RFC 1112
10) IGMP Version 2, No formal spec (see Appendix I of 11) below)
11) IGMP Version 3, Internet Draft
12) Distance Vector Multicast Routing Protocol, RFC 1075
13) Multicast Extensions to OSPF, RFC 1584
14) MOSPF: Analysis and Experience, RFC 1585
15) Protocol Independent Multicast (PIM): Protocol Specification (1/11/1995)
16) Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (9/7/95)

17) Resource Reservation Protocol (RSVP) -- Version 1 Functional Specification, Internet Draft (11/22/95)
18) Routing Support for RSVP, Internet Draft (6/30/95)
19) Border Gateway Protocol 4 (BGP-4), RFC 1771
20) OSPF Version 2, RFC 1583
21) A BGP/IDRP Route Server Alternative to a Full Mesh Routing, RFC 1863
22) Remote Network Monitoring Management Information Base (RMON), RFC 1757
23) 100 Mbps Fast Ethernet Specification, IEEE STD802.3u
24) Remote Authentication Dial In User Services (RADIUS), Internet Draft
25) ATM Forum User-Network Interface Specification, Version 3.1
26) BGP-4/IDRP for IP --- OSPF Interaction, RFC 1745

## *7.0 Technical Overview*[1]

### 7.1 @Home Network Architecture

@Home is a high-speed network that provides real-time multimedia news, information, entertainment and advertising content, access to the Internet, e-mail and other services to consumers via cable systems and their personal computers. The Mountain View, Calif.-based company is a joint venture between Tele-Communications Inc. (TCI), other major MSOs and independent cable system operators and the venture capital firm Kleiner Perkins Caufield & Byers.

The @Home network will provide consumers with a significant increase in speed and quality over current online connections. The service will use a customized version of the popular Netscape browser that will run on most Microsoft Windows, Windows 95, Macintosh OS and UNIX personal computers. @Home will employ an open platform architecture that will make its features available to the widest possible number of users and content providers. The @Home network will operate over a high-speed backbone and existing cable systems and will be linked to home computers via cable modems and standard Ethernet connections.

@Home's network is based on a distributed model (Figure 1) that makes extensive use of caching and replication to minimize traffic on the system's backbone and maintain high levels of speed. @Home will operate its own global network infrastructure connecting to the Internet at multiple NAP (Network Access Point) locations. The @Home backbone will connect regional networks together via a multi-megabit switched data system. These regional networks would serve major metropolitan areas, and would interconnect local servers located at Regional Data Centers (RDC) and cable system headends. @Home users would be connected to the headends via local area networks operating over the cable system, which is a two-way hybrid fiber-optic/coaxial cable configured asymmetrically. Many cable companies have upgraded their systems to handle such two-way connections or are in the process of doing so. In the home, a cable modem would interface between the cable plant and a local area ethernet network, to which the user PC is attached. The @Home backbone and regional networks would also serve tailsites, including content providers and @Work[2] customers.

@Home will include a wide variety of content. In addition to providing connections to the global Internet, the World Wide Web and e-mail, the service will enable content providers to create multimedia content that takes advantage of the high-speed network, as well as extensive local news and information.

---

[1] This section outlines @Home's plans for their network and is to be used for informational purposes only. The plans are subject to change as @Home's needs dictate.

[2] @Work is a division of @Home, that combines traditional ISP services for corporations (Internet access via leased lines) with @Home's high-bandwidth to the home, resulting in an attractive telecommuting option.

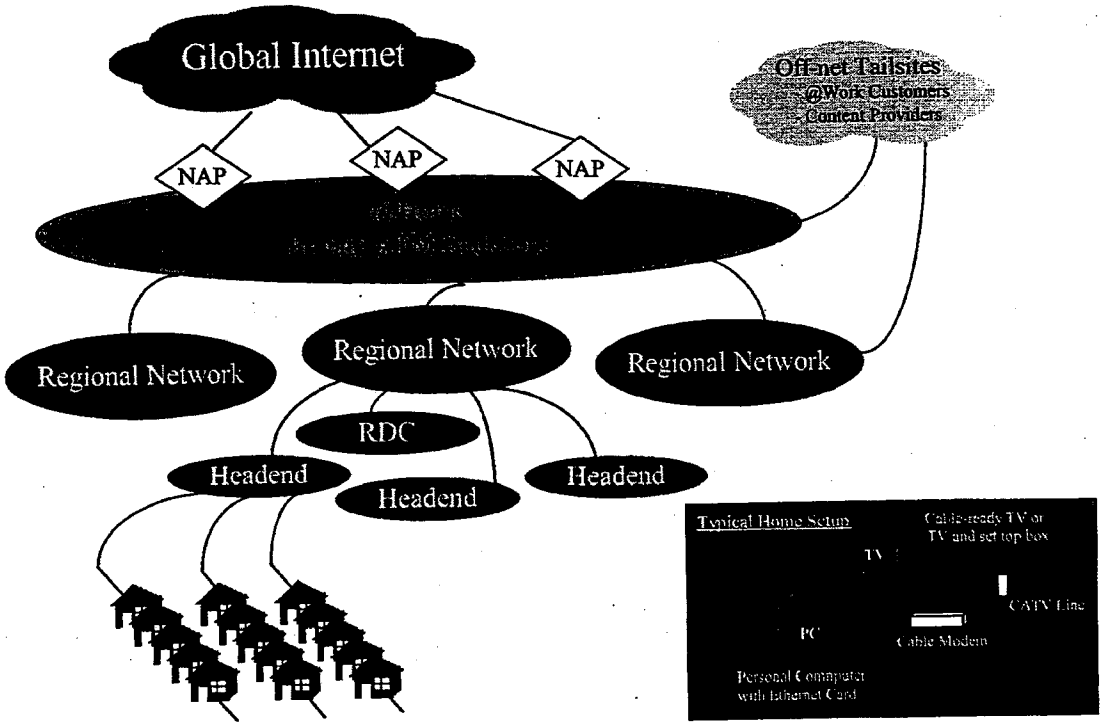


Figure 1: @Home Network Architecture

### 7.2 Backbone Network Subsystem

The @Home private backbone network (Figure 2) will be comprised of NAP/MAE routers, Regional Data Center (RDC) routers and tailsites interconnected via a nationwide ATM service (purchased from an Inter Exchange Carrier (IXC)).

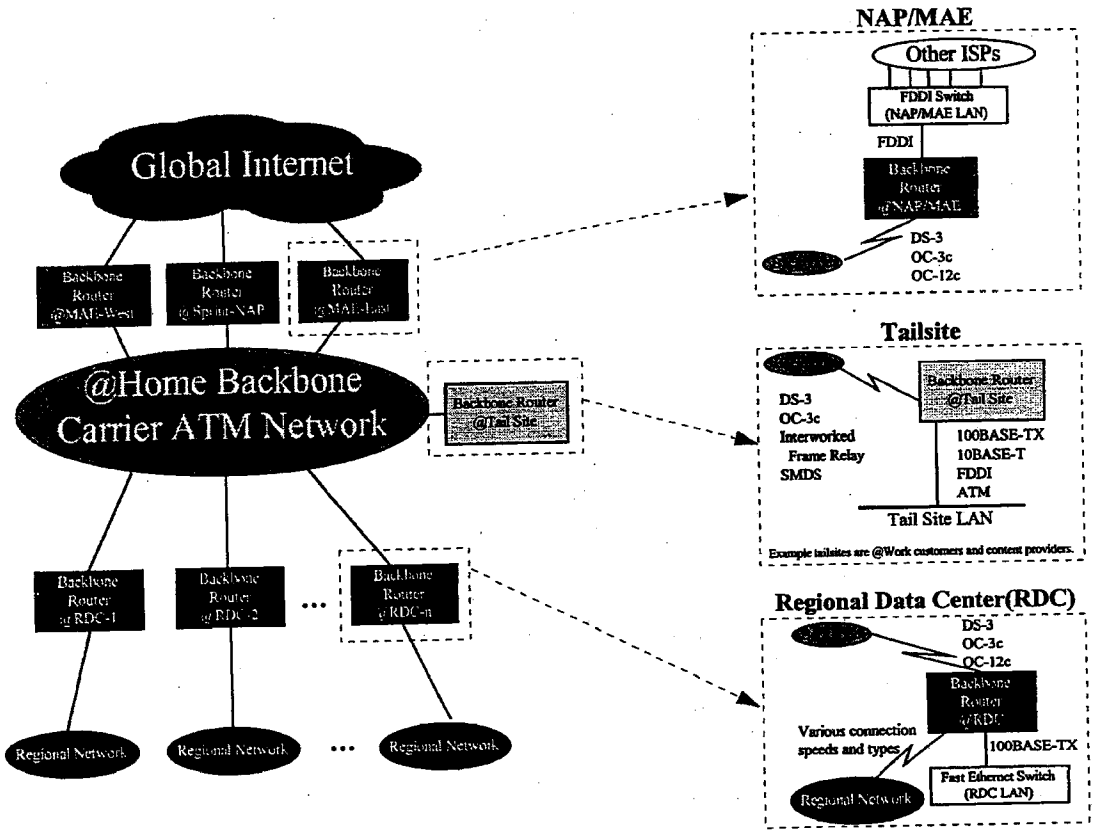


Figure 2: @Home Backbone Network Architecture

Initially, @Home will collocate their NAP/MAE routers at MAE-West (NASA/Ames, Moffett Field, CA), MAE-East (MFS Datanet, Washington, DC) and the Sprint-NAP (Pennsauken, NJ). For the Sunnyvale launch (April 1996), a single backbone router will also be located in a Regional Data Center in Santa Clara, CA. As the @Home service deploys nationwide, a NAP/MAE router will be collocated at other NAP/MAEs as they become populated. Similarly, backbone routers will be installed at RDCs as new geographic regions are brought up.

### *7.2.1 Backbone Routing*

Although the IGP and route redistribution method has yet to be finalized, current plans are for complete routing information (i.e. full routes) to be carried by all backbone routers. The @Home NAP/MAE routers will use BGP-4 as the EGP to peer with other ISPs. This introduces the problem of how to redistribute the 30,000+ external routes into the IGP. The two possible solutions under consideration for the backbone IGP are a) IBGP (Figure 3) or b) OSPF (Figure 4). Note that the IBGP solution utilizes Haskin's BGP/IDRP Route Server alternative (RFC 1863) to avoid the scaling problems of a full IBGP mesh. Vendors must outline the pros and cons of each approach, as well as other possible solutions. Based on this analysis, the vendor should propose an implementation, identifying proprietary components, where applicable.

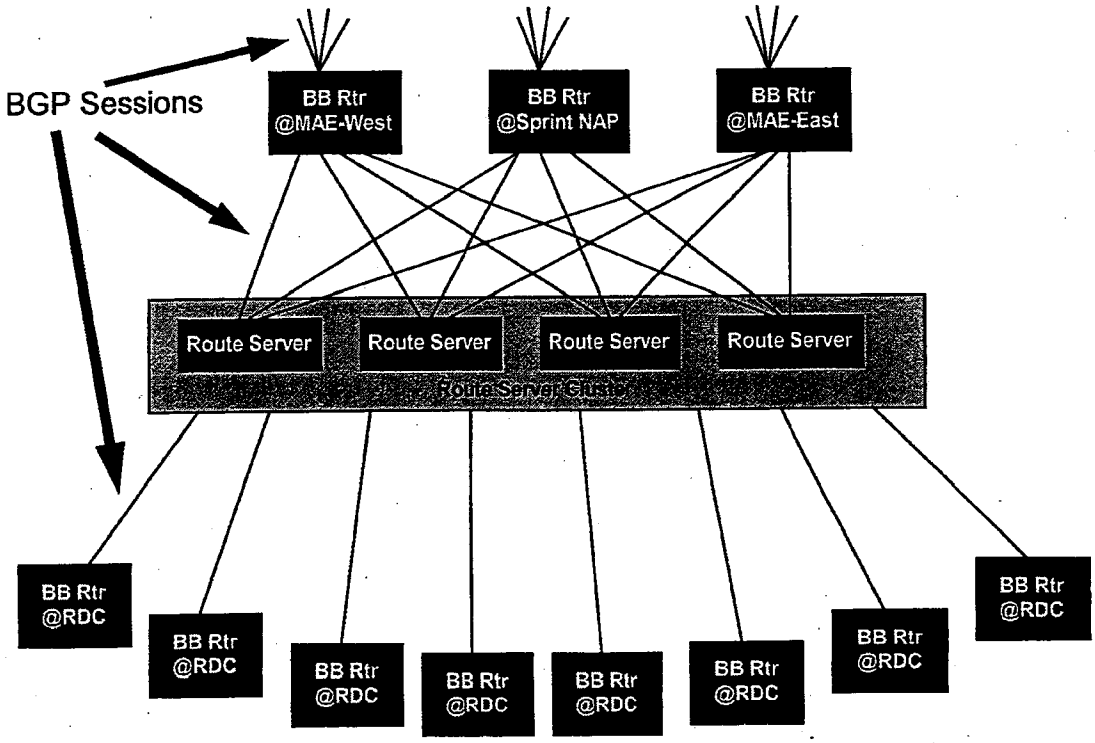


Figure 3: @Home Backbone Routing Architecture using BGP

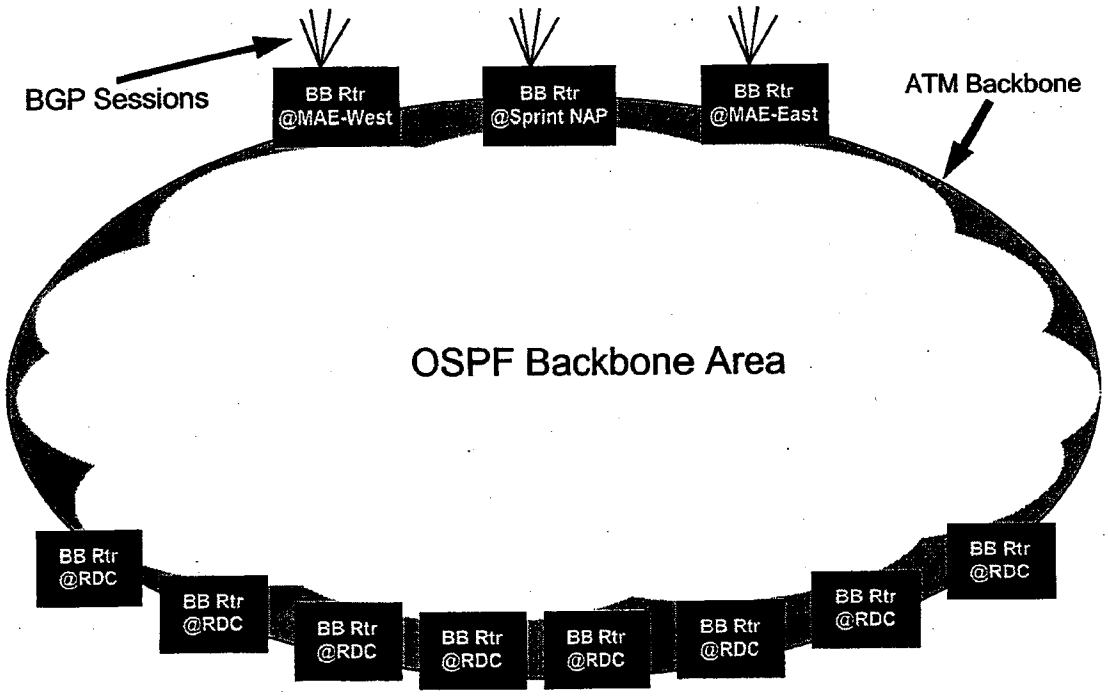


Figure 4: @Home Backbone Routing Architecture using OSPF

## 7.3 Regional Network Subsystem

The @Home regional networks (Figure 5) attach to the @Home backbone and interconnect Regional Data Centers (RDC), cable system headends and tailsites (e.g. @Work customers and content providers). The methods by which each location is attached to the regional network will vary. In many cases, @Home will have access to dark fiber throughout the region. A combination of switched (e.g. ATM) and dedicated (e.g. PPP over SONET) services will make the most efficient use of this dark fiber. Where dark fiber isn't available, traditional leased lines (e.g. DS-3 or OC-3c) will interconnect the regional sites. Though specifications are not outlined in this RFP, vendors may propose solutions which include ATM switching hardware in the regional network.

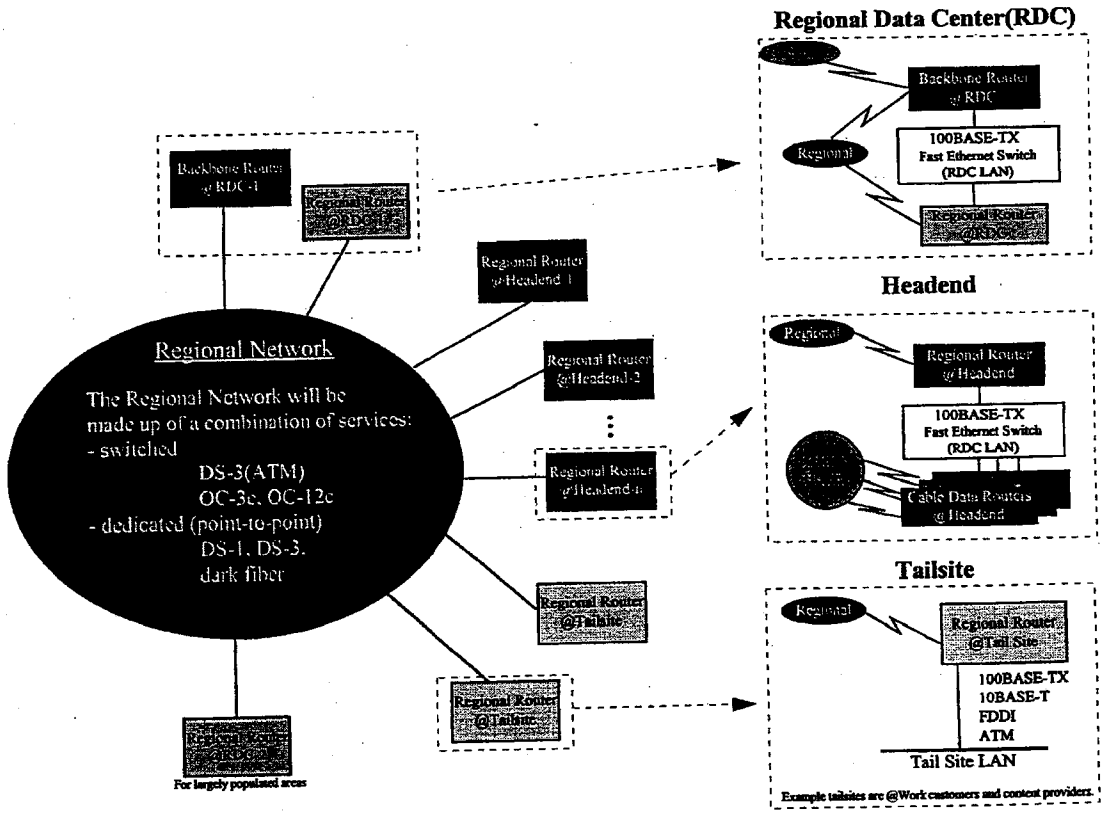


Figure 5: @Home Regional Network Architecture

## 7.4 Regional Data Center Switch Subsystem

An @Home Regional Data Center (RDC) houses high availability servers (for WWW, email, news, DHCP, etc.), high speed routers (linked to the backbone and regional networks) and a terminal server (for out-of-band access). All devices are connected by a 100BASE-TX Ethernet switch (Figure 6).

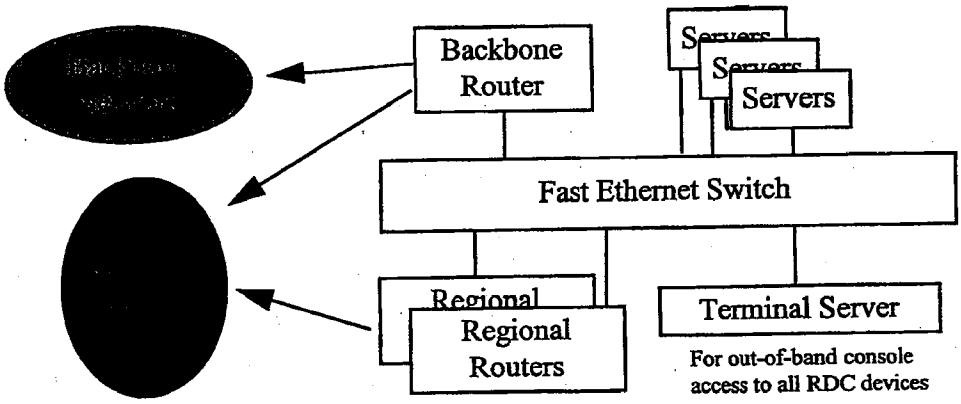


Figure 6: @Home Regional Data Center Architecture

### 7.5 Headend Switch Subsystem

At the cable headend facility, @Home will house WWW caching proxy servers, high speed routers (linked to the regional network) and a terminal server (for out-of-band access). All devices are connected by a 100BASE-TX Ethernet switch (Figure 7).

NOTE: Initially, some devices will be 10BASE-T Ethernet, transitioning to 100BASE-TX Ethernet by 1Q97.

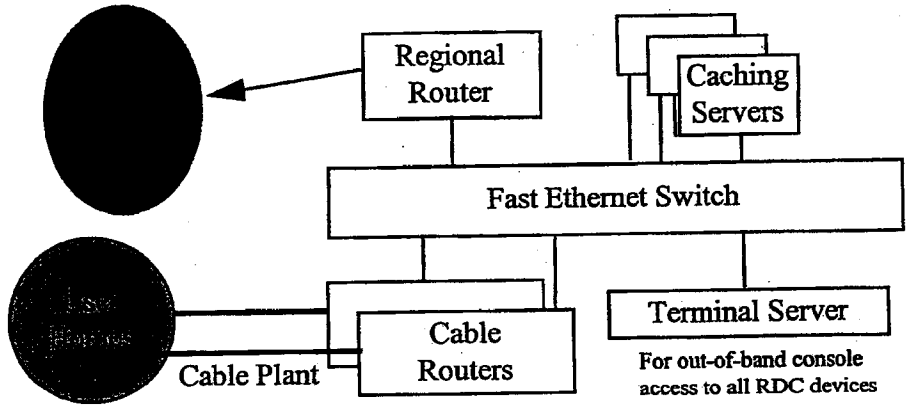


Figure 7: @Home Headend Architecture

## *8.0 Technical Requirements*

This section is separated into three parts: Backbone Network Subsystem (**8.1**), Regional Network Subsystem (**8.2**) and RDC and Headend Switch Subsystem (**8.3**). Each subsection lists requirements for the devices that make up each component of the network.

### 8.1 Backbone Network Subsystem

#### *8.1.1 Operations and Management*

*Load image and configuration*

**R:1** A device must have the ability to store multiple system images in local non-volatile storage, such as EEPROM or NVRAM.

R:2 A device must have the ability to load its system software over the network from a host or comparable device via TFTP or other protocol.

R:3 A device must have a mechanism to allow "failover" to an alternate method of loading its system software, in the event the primary method isn't available or has failed.

R:4 A device must perform some basic consistency check on any image loaded, to detect and perhaps prevent corrupted images.

R:5 A device must have the ability to store multiple configurations in local non-volatile storage, such as EEPROM or NVRAM.

R:6 A device must have the ability to load its configurations over the network from a host or comparable device via TFTP or other protocol. While offline, the configuration must be stored in ASCII formatted text file, to which comments can be inserted and maintained.

R:7 A device must implement a mechanism for dumping the contents of its memory (and/or state useful for vendor debugging after a crash), and saving them on another host via an up-line dump mechanism such as TFTP or FTP.

R:8 A device must implement a mechanism for detecting and responding to misconfigurations. If a command is executed incorrectly, the device should give an error message. The device should not accept a poorly formed command. It is understood that a command that is correctly formatted may result in misconfiguration with respect to the network. We don't expect the device to "do what I mean, not what I say".

*Security Enhancements*

R:9 A device must have the ability to filter traffic destined for the device by source address. This filter applies across all existing (and future) services.

R:10 All network services on the device must be able to run on any (TCP/UDP) port number. For example, Telnet listens on port 50 instead of the default port 23.

*In-Band Access*

R:11 The device must provide In-Band access. In-band access primarily refers to access through normal network protocols that may or may not affect the permanent operational state of the device. This includes, but is not limited to, encrypted Telnet/RLOGIN console access and SNMP operations. This access must implement access controls (including, but not limited to, one-time passwords), to prevent unauthorized access.

*Out-of-Band Access*

R:12 The device must support Out-Of-Band (OOB) access. This access must provide the same functionality as in-band access. This access must implement access controls, to prevent unauthorized access. The physical interface (console port) on the device should support full modem control ands speeds up to at lest 9600 bps.

R:13 Out-of-Band access must use RADIUS for authentication. In the event the network (and RADIUS server) is unreachable, authentication should failover to preconfigured, locally stored usernames and passwords.

*User Interface*

R:14 A device must implement a single command line interface with a management hierarchy to allow privileged and non-privileged access to the configuration. In addition to the command line interface, vendors may implement application-based programs to aid device configuration and management.

*Control*

**R:15** Each device has configuration parameters that may need to be set. It must be possible to update the parameters without rebooting (cold start) the device; at worst, a restart (warm start) may be required.

**R:16** A means must be provided, either as an application program or a device function, to modify parameters on-line and offline (to be archived or uploaded after modifications).

**R:17** A device must include both in-band and out-of-band mechanisms to allow the network manager to reload, stop and restart the device. It must also contain a mechanism (such as a watchdog timer) which will reboot the device automatically if it hangs due to a software or hardware fault.

*Loopback*

**R:18** Software loopback capability on a per interface basis and on a per PVC basis for cloud services such as ATM.

*Troubleshooting*

**R:19** Syslog and/or debug interface. This would allow the operator to capture debugging information on the console or save it offline.

**R:20** The device must have the ability to initiate an ICMP echo (ping) with a complement of options, such as packet size, data pattern, repeat count, etc.

**R:21** The device must have the ability to initiate a traceroute with a complement of options, such as source address, waittime, max TTL, etc.

**R:22** The device must have the ability to initiate Telnet sessions.

*SNMP Support*

**R:23** The device must have full SNMP agent installation (i.e. it can be polled) with the ability to send standard and customized traps.

**R:24** The device must have re-mapping capabilities to run SNMP on a non-standard port.

**R:25** On a per community basis, the device must have the ability to set configuration parameters via SNMP.

**R:26** On a per community basis, the device must have the ability to disable SNMP sets, without disabling SNMP gets.

**R:27** The device must have the ability to configure multiple community name/trusted host pairs (allowing traps to be sent to different hosts - not just a single, central NMS).

**R:28** The vendor must provide MIBs for all supported protocols and interfaces.

**R:29** The vendor must provide an environmental (power, temperature, etc.,) monitor that is SNMP-readable.

**R:30** The vendor must demonstrate commitment to implement SNMPv2.

**R:31** The vendor must demonstrate commitment to implement SNMPv2 Security.

**R:32** The vendor must demonstrate commitment to implement RMON2.

*Accounting*

**R:33** The device must provide a method for auditing configuration modifications.

**R:34** The device must provide a method for auditing security related events, such as authorization failures/approvals, violations of policy control and SNMP-probing.

R:35 The device must provide a method for tracking traffic levels between pairs of hosts or networks. A mechanism for limiting the scope of this accounting is required.

### *8.1.2 Powering*

*Input*

R:36 The device will be powered with the following input specifications.

Voltage 120 V AC +/-10%
Frequency 57 Hz to 63 Hz

*Power Consumption*

R:37 Specify the power consumption of the device.

### *8.1.3 Physical Requirements*

*Form Factor, Mounting*

R:38 Space is limited in the operational facilities. The device and associated cables will need to be mounted in 19" wide by 24" deep communications racks. Specify the height of the device in inches. Additional consideration will be given to systems with high port density per inch of rack space.

*Physical Description*

R:39 Specify the physical size of the fully equipped system. Note all access points, and physical cable entry and exit points.

*Ventilation and Cooling*

R:40 Specify the ventilation and spacing requirements.

### *8.1.4 Operational Characteristics*

*Heat Dissipation*

R:41 Specify the heat dissipation of server in BTU per hour.

*Operating Temperature, Humidity*

R:42 0 to 40 degrees C, 85% non-condensing humidity.

*Altitude*

R:43 Sea level to 12,000 ft (3,658 M) above sea level.

*Electrical and Environmental regulatory compliance*

R:44 The device must comply with all applicable local, state, and federal regulations regarding electrical emissions and shielding, and electrical and environmental safety.

### *8.1.5 Router Performance and Functionality*

R:45 Operating with a configuration that meets all the requirements outlined in this RFP, the router must forward, at wire speed, packets of length 64 bytes on all interfaces.

*RFC 1812 compliance*

RFC 1812 ("Requirements for IP Version 4 Routers") outlines requirements that @Home expects all router solutions to meet.

**R:46** The router must be *conditionally compliant* (as defined in the document) with RFC 1812. If this level of conformance is not met, router vendors are asked to list issues not supported, reasons for nonconformance, future plans and timelines. [Section 1.1.3]

**R:47** The router should be *unconditionally compliant* (as defined in the document) with RFC 1812. If this level of conformance is not met, router vendors are asked to list issues not supported, reasons for nonconformance, future plans and timelines. [Section 1.1.3]

Particular issues which are listed in the RFC as "SHOULD" implement, but which @Home require include

*Type Of Service (TOS)*

**R:48** The router must support priority-based queueing. [Section 5.3.3]

**R:49** Traffic priority must be identified by the precedence bits within the TOS byte in the IP header.

**R:50** The router must have the ability to modify (set or clear) the precedence bits in the TOS byte of the IP header, on a per interface basis.

**R:51** The vendor must describe the performance impact of **R:48, R:49** and **R:50** when the features are enabled and in use.

**R:52** The vendor must demonstrate commitment to implement RSVP.

*Multicast*

**R:53** The router must satisfy the Host Requirements with respect to IP multicasting, as specified in RFC 1122. This implies support for all of RFC 1112 including IGMP. [Section 4.2.3.2]

**R:54** The router must implement the multicast router portion of IGMP. [Section 5.2.8]

**R:55** The router must implement the following multicast routing protocols: DVMRP with pruning support (as implemented in mrouted v3.5), PIM-SM, PIM-DM and MOSPF.

**R:56** The vendor must provide a multicast protocol strategy for the @Home network. Vendors must discuss the suitability of their solution at each level (Backbone, Regional, RDC and Headend) of the network.

*Filters*

**R:57** As a means of providing security and/or limiting traffic through portions of a network, at a minimum, a router must provide the ability to selectively forward (or filter) packets based on any combination of: source address, destination address, source port or destination port. Provide details on packet filtering capabilities. [Section 5.3.9]

**R:58** The router must provide some priority mechanism for choosing routes from independent routing processes. Routers must provide control of IGP-IGP exchange. Routers must provide some mechanism for translating or transforming metrics on a per network basis. [Section 7.6]

**R:59** The vendor must describe the performance impact of **R:56** and **R:57** when the features are enabled and in use.

### *8.1.6 Routing Protocols*

**R:60** The router must implement Open Shortest Path First (OSPF). [Section 7.2.2]

**R:61** The router must implement Border Gateway Protocol (BGP-4). [Section 7.3.2]

**R:62** The router must implement Routing Information Protocol (RIP, preferably v2).

**R:63** The Vendor should show how their implementation of each of these protocols will scale to a system that carries a large number of routes (on the order of 30,000).

**R:64** The vendor must describe how routes are distributed between routing protocols within the router and what controls are available to control the redistribution.

**R:65** The vendor must demonstrate compliance with RFC1745 "BGP-4/IDRP for IP — OSPF Interaction".

#### *Miscellaneous Protocols*

**R:66** The router must provide BOOTP relay-agent capability. [Section 9.1.2]

### *8.1.7 Router Interfaces*

**R:67** Interface that has the ability to light single mode dark fiber across medium (< 20Km) and long (> 20 Km) range distances. It must operate at a minimum speed of 45Mbps. For example, this could be a SONET interface with PPP.

**R:68** Native ATM, operating on DS-3, OC-3c and OC-12c interfaces.

**R:69** ATM forum UNI 3.1 and appropriate PLCPs must be supported.

**R:70** PPP operating on DS-3, OC-3c and OC-12c interfaces.

**R:71** HSSI, operating at speeds up to 52Mbps.

**R:72** Full duplex FDDI, operating at speeds up to 100Mbps.

**R:73** 100BASE-TX Full Duplex Ethernet, operating at speeds up to 100Mbps.

### *8.1.8 NAP/MAE Router Proof of concept*

**R:74** As the NAP/MAE routers will be peering with other Tier 1 ISPs, the number of routes it must process is very large. If the vendor proposes a solution in this area, they must provide detailed evidence to demonstrate their ability to operate in such an environment. This includes citing examples of ISPs using their product, attached to a NAP/MAE and peering, and exchanging routes, with a large number of Tier 1 ISPs.

**R:75** Route flapping is a severe problem at major interconnect points like the NAP/MAEs. The vendor must describe their implementations of flap dampening algorithms.

### 8.2 Regional Network Subsystem

#### *8.2.1 Operations and Management*

*Load image and configuration*

**R:76** A device must have the ability to store multiple system images in local non-volatile storage, such as EEPROM or NVRAM.

**R:77** A device must have the ability to load its system software over the network from a host or comparable device via TFTP or other protocol.

**R:78** A device must have a mechanism to allow "failover" to an alternate method of loading its system software, in the event the primary method isn't available or has failed.

**R:79** A device must perform some basic consistency check on any image loaded, to detect and perhaps prevent corrupted images.

**R:80** A device must have the ability to store multiple configurations in local non-volatile storage , such as EEPROM or NVRAM.

**R:81** A device must have the ability to load its configurations over the network from a host or comparable device via TFTP or other protocol. While offline, the configuration must be stored in ASCII formatted text file, to which comments can be inserted and maintained.

**R:82** A device must implement a mechanism for dumping the contents of its memory (and/or state useful for vendor debugging after a crash), and saving them on another host via an up-line dump mechanism such as TFTP or FTP.

**R:83** A device must implement a mechanism for detecting and responding to misconfigurations. If a command is executed incorrectly, the device should give an error message. The device should not accept a poorly formed command. It is understood that a command that is correctly formatted may result in misconfiguration with respect to the network. We don't expect the device to "do what I mean, not what I say".

*Security Enhancements*

**R:84** A device must have the ability to filter traffic destined for the device by source address. This filter applies across all existing (and future) services.

**R:85** All network services on the device must be able to run on any (TCP/UDP) port number. For example, Telnet listens on port 50 instead of the default port 23.

*In-Band Access*

**R:86** The device must provide In-Band access. In-band access primarily refers to access through normal network protocols that may or may not affect the permanent operational state of the device. This includes, but is not limited to, encrypted Telnet/RLOGIN console access and SNMP operations. This access must implement access controls (including, but not limited to, one-time passwords), to prevent unauthorized access.

*Out-of-Band Access*

**R:87** The device must support Out-Of-Band (OOB) access. This access must provide the same functionality as in-band access. This access must implement access controls, to prevent unauthorized access. The physical interface (console port) on the device should support full modem control ands speeds up to at lest 9600 bps.

**R:88** Out-of-Band access must use RADIUS for authentication. In the event the network (and RADIUS server) is unreachable, authentication should failover to preconfigured, locally stored usernames and passwords

*User Interface*

**R:89** A device must implement a single command line interface with a management hierarchy to allow privileged and non-privileged access to the configuration. In addition to the command line interface, vendors may implement application-based programs to aid device configuration and management.

*Control*

**R:90** Each device has configuration parameters that may need to be set. It must be possible to update the parameters without rebooting (cold start) the device; at worst, a restart (warm start) may be required.

**R:91** A means must be provided, either as an application program or a device function, to modify parameters on-line and offline (to be archived or uploaded after modifications).

**R:92** A device must include both in-band and out-of-band mechanisms to allow the network manager to reload, stop and restart the device. It must also contain a mechanism (such as a watchdog timer) which will reboot the device automatically if it hangs due to a software or hardware fault.

*Loopback*

**R:93** Software loopback capability on a per interface basis and on a per PVC basis for cloud services such as ATM.

*Troubleshooting*

**R:94** Syslog and/or debug interface. This would allow the operator to capture debugging information on the console or save it offline.

**R:95** The device must have the ability to initiate an ICMP echo (ping) with a complement of options, such as packet size, data pattern, repeat count, etc.,

**R:96** The device must have the ability to initiate a traceroute with a complement of options,, such as source address, waittime, max TTL, etc.,

**R:97** The device must have the ability to initiate Telnet sessions.

*SNMP Support*

**R:98** The device must have full SNMP agent installation (i.e. it can be polled) with the ability to send standard and customized traps.

**R:99** The device must have re-mapping capabilities to run SNMP on a non-standard port.

**R:100** On a per community basis, the device must have the ability to set configuration parameters via SNMP.

**R:101** On a per community basis, the device must have the ability to disable SNMP sets, without disabling SNMP gets.

**R:102** The device must have the ability to configure multiple community name/trusted host pairs (allowing traps to be sent to different hosts - not just a single, central NMS).

**R:103** The vendor must provide MIBs for all supported protocols and interfaces.

**R:104** The vendor must provide an environmental (power, temperature, etc.,) monitor that is SNMP-readable.

**R:105** The vendor must demonstrate commitment to implement SNMPv2.

**R:106** The vendor must demonstrate commitment to implement SNMPv2 Security.

**R:107** The vendor must demonstrate commitment to implement RMON2.

*Accounting*

**R:108** The device must provide a method for auditing configuration modifications.

**R:109** The device must provide a method for auditing security related events, such as authorization failures/approvals, violations of policy control and SNMP-probing.

**R:110** The device must provide a method for tracking traffic levels between pairs of hosts or networks. A mechanism for limiting the scope of this accounting is required.

### *8.2.2 Powering*

*Input*

**R:111** The device will be powered with the following input specifications.

Voltage 120 V AC +/-10%
Frequency 57 Hz to 63 Hz

*Power Consumption*

**R:112** Specify the power consumption of the device.

### *8.2.3 Physical Requirements*

*Form Factor, Mounting*

**R:113** Space is limited in the operational facilities. The device and associated cables will need to be mounted in 19" wide by 24" deep communications racks. Specify the height of the device in inches. Additional consideration will be given to systems with high port density per inch of rack space.

*Physical Description*

**R:114** Specify the physical size of the fully equipped system. Note all access points, and physical cable entry and exit points.

*Ventilation and Cooling*

**R:115** Specify the ventilation and spacing requirements.

### *8.2.4 Operational Characteristics*

*Heat Dissipation*

**R:116** Specify the heat dissipation of server in BTU per hour.

*Operating Temperature, Humidity*

**R:117** 0 to 40 degrees C, 85% non-condensing humidity.

*Altitude*

**R:118** Sea level to 12,000 ft (3,658 M) above sea level.

*Electrical and Environmental regulatory compliance*

**R:119** The device must comply with all applicable local, state, and federal regulations regarding electrical emissions and shielding, and electrical and environmental safety.

### *8.2.5 Router Performance and Functionality*

**R:120** Operating with a configuration that meets all the requirements outlined in this RFP, the router must forward, at wire speed, packets of length 64 bytes on all interfaces.

*RFC 1812 compliance*

RFC 1812 ("Requirements for IP Version 4 Routers") outlines requirements that @Home expects all router solutions to meet.

**R:121** The router must be *conditionally compliant* (as defined in the document) with RFC 1812. If this level of conformance is not met, router vendors are asked to list issues not supported, reasons for nonconformance, future plans and timelines. [Section 1.1.3]

**R:122** The router should be *unconditionally compliant* (as defined in the document) with RFC 1812. If this level of conformance is not met, router vendors are asked to list issues not supported, reasons for nonconformance, future plans and timelines. [Section 1.1.3]

Particular issues which are listed in the RFC as "SHOULD" implement, but which @Home require include

*Type Of Service (TOS)*

**R:123** The router must support priority-based queueing. [Section 5.3.3]

**R:124** Traffic priority must be identified by the precedence bits within the Type Of Service (TOS) byte in the IP header.

**R:125** The router must have the ability to modify (set or clear) the precedence bits in the TOS byte of the IP header, on a per interface basis.

**R:126** The vendor must describe the performance impact of **R:122**, **R:123** and **R:124** when the features are enabled and in use.

**R:127** The vendor must demonstrate commitment to implement RSVP.

*Multicast*

**R:129** The router must satisfy the Host Requirements with respect to IP multicasting, as specified in RFC 1122. This implies support for all of RFC 1112 including IGMP. [Section 4.2.3.2]

**R:130** The router must implement the multicast router portion of IGMP. [Section 5.2.8]

**R:131** The router must implement the following multicast routing protocols: DVMRP with pruning support (as implemented in mrouted v3.5), PIM-SM, PIM-DM and MOSPF.

**R:132** The vendor must provide a multicast protocol strategy for the @Home network. Vendors must discuss the suitability of their solution at each level (Backbone, Regional, RDC and Headend) of the network.

*Filters*

**R:133** As a means of providing security and/or limiting traffic through portions of a network, at a minimum, a router must provide the ability to selectively forward (or filter) packets based on any combination of: source address, destination address, source port or destination port. Provide details on packet filtering capabilities. [Section 5.3.9]

**R:134** The router must provide some priority mechanism for choosing routes from independent routing processes. Routers must provide control of IGP-IGP exchange. Routers must provide some mechanism for translating or transforming metrics on a per network basis.[Section 7.6]

**R:135** The vendor must describe the performance impact of **R:131** and **R:132** when the features are enabled and in use.

### *8.2.6 Routing Protocols*

**R:136** The router must implement Open Shortest Path First (OSPF). [Section 7.2.2]

**R:137** The router must implement Border Gateway Protocol (BGP-4). [Section 7.3.2]

**R:138** The router must implement Routing Information Protocol (RIP, preferably v2).

**R:139** The Vendor should show how their implementation of each of these protocols will scale to a system that carries a large number of routes (on the order of 30,000).

**R:140** The vendor must describe how routes are distributed between routing protocols within the router and what controls are available to control the redistribution.

**R:141** The vendor must demonstrate compliance with RFC1745 "BGP-4/IDRP for IP — OSPF Interaction".

***Miscellaneous Protocols***

**R:142** The router must provide BOOTP relay-agent capability. [Section 9.1.2]

### *8.2.7 Router Interfaces*

**R:143** Interface that has the ability to light single mode dark fiber across medium (< 20Km) and long (> 20 Km) range distances. It must operate at a minimum speed of 45Mbps. For example, this could be a SONET interface with PPP.

**R:144** Native ATM, operating on DS-3, OC-3c and OC-12c interfaces.

**R:145** ATM forum UNI 3.1 and appropriate PLCPs must be supported.

**R:146** PPP operating on DS-3, OC-3c and OC-12c interfaces.

**R:147** HSSI, operating at speeds up to 52Mbps.

**R:148** Serial Interface, operating at speeds up to T-1 using PPP.

**R:149** Frame Relay, operating at speeds up to T-3.

**R:150** SMDS, operating at speeds up to 34Mbps.

**R:151** Channelized T3, allowing multiple T1s to be supported via single physical interface, supporting up to 28 T1s.

**R:152** Full duplex FDDI, operating at speeds up to 100Mbps.

**R:153** 100BASE-TX Full Duplex Ethernet, operating at speeds up to 100Mbps.

## 8.3 RDC and Headend Switch Subsystem

### *8.3.1 Operations and Management*

*Load image and configuration*

**R:154** A device must have the ability to store multiple system images in local non-volatile storage, such as EEPROM or NVRAM.

**R:155** A device must have the ability to load its system software over the network from a host or comparable device via TFTP or other protocol.

**R:156** A device must have a mechanism to allow "failover" to an alternate method of loading its system software, in the event the primary method isn't available or has failed.

**R:157** A device must perform some basic consistency check on any image loaded, to detect and perhaps prevent corrupted images.

**R:158** A device must have the ability to store multiple configurations in local non-volatile storage , such as EEPROM or NVRAM.

**R:159** A device must have the ability to load its configurations over the network from a host or comparable device via TFTP or other protocol. While offline, the configuration must be stored in ASCII formatted text file, to which comments can be inserted and maintained.

**R:160** A device must implement a mechanism for dumping the contents of its memory (and/or state useful for vendor debugging after a crash), and saving them on another host via an up-line dump mechanism such as TFTP or FTP.

**R:161** A device must implement a mechanism for detecting and responding to misconfigurations. If a command is executed incorrectly, the device should give an error message. The device should not accept a poorly formed command. It is understood that a command that is correctly formatted may result in misconfiguration with respect to the network. We don't expect the device to "do what I mean, not what I say".

*Security Enhancements*

**R:162** A device must have the ability to filter traffic destined for the device by source address. This filter applies across all existing (and future) services.

**R:163** All network services on the device must be able to run on any (TCP/UDP) port number. For example, Telnet listens on port 50 instead of the default port 23.

*In-Band Access*

**R:164** The device must provide In-Band access. In-band access primarily refers to access through normal network protocols that may or may not affect the permanent operational state of the device. This includes, but is not limited to, encrypted Telnet/RLOGIN console access and SNMP operations. This access must implement access controls (including, but not limited to, one-time passwords), to prevent unauthorized access.

*Out-of-Band Access*

**R:165** The device must support Out-Of-Band (OOB) access. This access must provide the same functionality as in-band access. This access must implement access controls, to prevent unauthorized access. The physical interface (console port) on the device should support full modem control ands speeds up to at lest 9600 bps.

**R:166** Out-of-Band access must use RADIUS for authentication. In the event the network (and RADIUS server) is unreachable, authentication should failover to preconfigured, locally stored usernames and passwords.

*User Interface*

**R:167** A device must implement a single command line interface with a management hierarchy to allow privileged and non-privileged access to the configuration. In addition to the command line interface, vendors may implement application-based programs to aid device configuration and management.

*Control*

**R:168** Each device has configuration parameters that may need to be set. It must be possible to update the parameters without rebooting (cold start) the device; at worst, a restart (warm start) may be required.

**R:169** A means must be provided, either as an application program or a device function, to modify parameters on-line and offline (to be archived or uploaded after modifications).

**R:170** A device must include both in-band and out-of-band mechanisms to allow the network manager to reload, stop and restart the device. It must also contain a mechanism (such as a watchdog timer) which will reboot the device automatically if it hangs due to a software or hardware fault.

*Loopback*

**R:171** Software loopback capability on a per interface basis and on a per PVC basis for cloud services such as ATM.

*Troubleshooting*

**R:172** Syslog and/or debug interface. This would allow the operator to capture debugging information on the console or save it offline.

**R:173** The device must have the ability to initiate an ICMP echo (ping) with a complement of options, such as packet size, data pattern, repeat count, etc.,

**R:174** The device must have the ability to initiate a traceroute with a complement of options,, such as source address, waittime, max TTL, etc.,

**R:175** The device must have the ability to initiate Telnet sessions.

*SNMP Support*

**R:176** The device must have full SNMP agent installation (i.e. it can be polled) with the ability to send standard and customized traps.

**R:177** The device must have re-mapping capabilities to run SNMP on a non-standard port.

**R:178** On a per community basis, the device must have the ability to set configuration parameters via SNMP.

**R:179** On a per community basis, the device must have the ability to disable SNMP sets, without disabling SNMP gets.

**R:180** The device must have the ability to configure multiple community name/trusted host pairs (allowing traps to be sent to different hosts - not just a single, central NMS).

**R:181** The vendor must provide MIBs for all supported protocols and interfaces.

**R:182** The vendor must provide an environmental (power, temperature, etc.,) monitor that is SNMP-readable.

**R:183** The vendor must demonstrate commitment to implement SNMPv2.

**R:184** The vendor must demonstrate commitment to implement SNMPv2 Security.

**R:185** The vendor must demonstrate commitment to implement RMON2.

*Accounting*

**R:186** The device must provide a method for auditing configuration modifications.

**R:187** The device must provide a method for auditing security related events, such as authorization failures/approvals, violations of policy control and SNMP-probing.

**R:188** The device must provide a method for tracking traffic levels between pairs of hosts or networks. A mechanism for limiting the scope of this accounting is required.

### *8.3.2 Powering*

*Input*

**R:189** The device will be powered with the following input specifications.

Voltage 120 V AC +/-10%
Frequency 57 Hz to 63 Hz

*Power Consumption*

**R:190** Specify the power consumption of the device.

### *8.3.3 Physical Requirements*

*Form Factor, Mounting*

**R:191** Space is limited in the operational facilities. The device and associated cables will need to be mounted in 19" wide by 24" deep communications racks. Specify the height of the device in

inches. Additional consideration will be given to systems with high port density per inch of rack space.

*Physical Description*

**R:192** Specify the physical size of the fully equipped system. Note all access points, and physical cable entry and exit points.

*Ventilation and Cooling*

**R:193** Specify the ventilation and spacing requirements.

### *8.3.4 Operational Characteristics*

*Heat Dissipation*

**R:194** Specify the heat dissipation of server in BTU per hour.

*Operating Temperature, Humidity*

**R:195** 0 to 40 degrees C, 85% non-condensing humidity.

*Altitude*

**R:196** Sea level to 12,000 ft (3,658 M) above sea level.

*Electrical and Environmental regulatory compliance*

**R:197** The device must comply with all applicable local, state, and federal regulations regarding electrical emissions and shielding, and electrical and environmental safety.

### *8.3.5 Switch Functionality and Performance*

**R:198** All ports must be switched.

**R:199** The switch must be non-blocking for unicast traffic.

**R:200** The switch must forward, at wire speed, packets of length 64 bytes.

**R:201** Must conform to the IEEE Std 802.3u. The vendor must provide a copy of the "Implementation Conformance Statement" (PICS) showing which features and options of the standard have been implemented.

***Troubleshooting***

**R:202** To facilitate network troubleshooting, one port should be able to clone traffic from any other port on the switch.

**R:203** Support of the "Remote Network Monitoring MIB", RFC1757 is required. The vendor must conform to the entire MIB.

***Multicast***

**R:204** To prevent inefficient use of network bandwidth, received IP multicast packets must not be unconditionally flooded out all ports.. Instead, the switch must learn, on a per interface basis, the location of IP multicast group members, such that, when a IP multicast packet arrives at the switch, it is only forwarded out interfaces leading to members of that specific IP multicast group.

### *8.3.6 Switch Interfaces*

**R:205** Each port must support 100BASE-TX Full Duplex Ethernet and 10BASE-T Ethernet with the appropriate speed determined by the Fast Ethernet auto-negotiation option.